≡



VK.com

VK is the largest European social network with more than a 100 million active users.

https://vk.com · @vkontakte

Reports resolved	Assets in scope	Average bounty
841	14	-

Bug Bounty Program

Launched on May 2015

Includes retesting ⓘ **Bounty splitting enabled** ⓘ

Policy Hacktivity Thanks Updates (0) Collaborators

Rewards

Low	Medium	High	Critical
$500	$1,000	$5,000	$15,000

Detailed Rewards

Our bounty range is **$100 - $15,000** USD.

Reward amounts may vary depending upon the severity, novelty, difficulty to exploit, and impact of the vulnerability reported. The following table is a reference for the average rewards of specific classes of vulnerabilities.

Vulnerability	Bounty for Critical Assets	All Others
Remote Code Execution (RCE), server-side	$15,000	$5,000
Remote Code Execution (RCE), mobile app	$3,000	$1,000
SQL Injection (SQLi)	$10,000	$3,000
Local/Remote File Inclusion (LFI, RFI)	$5,000	$2,000
XML External Entity (XXE)	$5,000	$2,000
Server-Side Request Forgery (SSRF)	$5,000	$1,000
Server-Side Request Forgery (SSRF), blind	$1,000	$500

Cross-Site Scripting (XSS)	$500	$300
Open Redirect	$300	$100

For more information, see the **Policy** section.

Last updated on July 2, 2020. View changes

Policy

For English description, see below.

Программа поиска уязвимостей VK.com

Программа ограничена поиском технических уязвимостей в сервисах компании и в ее официальных мобильных приложениях.

Уязвимости — недостатки в системе, использование которых может намеренно нарушить её целостность, конфиденциальность или вызвать неправильную работу.

По вопросам, не относящимся к данной программе, стоит обращаться в нашу службу Поддержки.

Официальные сообщества приложений:

- ВКонтакте для iPhone: https://vk.com/iphone_app
- ВКонтакте для Android: https://vk.com/android_app
- VK Admin: https://vk.com/vkadmin
- VK Messenger: https://vk.com/desktop_app

Принимаем в качестве уязвимостей:

В качестве классификации уязвимостей для веб-сервисов используется OWASP Top 10 2017 года, для мобильных приложений — OWASP Mobile Top 10 2016 года.

- Remote Code Execution (RCE)
- SQL Injection
- Local-Remote File Inclusion (LFI/RFI)
- XML External Entity (XXE)
- Broken Authentication (обход 2FA, и т.д.)
- Sensitive Data Exposure
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Using Components with Known Vulnerabilities (с примерами)
- Server Side Request Forgery (SSRF)
- Cross Site Request Forgery (CSRF)
- Insecure Direct Object References (IDOR)

- Other Injections

Не принимаем:

- Сообщения от сканеров безопасности и других автоматических систем.
- Сообщения об уязвимости, основанные на версиях ПО/протокола, без указания реального применения.
- Сообщения об отсутствии механизма защиты или несоответствия рекомендациям (например, отсутствие CSRF токена) без указания на реально существующие негативные последствия.
- Logout CSRF.
- Self-XSS.
- Framing.
- Clickjacking.
- Сообщения об Open Redirect (через /away.php).
- Гомографические атаки IDN.
- Раскрытие публичной информации о пользователе/сообществе (см. настройки приватности).
- Атаки, требующие полного доступа к странице пользователя или профилю браузера.
- Уязвимости в партнерских сервисах и продуктах, которые непосредственно не затрагивают безопасность сервисов компании.

Строго запрещены:

- DDoS атаки.
- Социальная инженерия.
- Получение физического доступа к серверам/инфраструктуре.
- Угрозы/причинение вреда сотрудникам компании.

Более того, подобные действия будут преследоваться по закону.

Пожелания к отчету:

Следование этому пожеланию увеличит вероятность получения награды.

- Сервис, в котором найдена уязвимость.
- Тип уязвимости.
- Примеры эксплуатации со скриншотами/скринкастом.
- Способы воспроизведения.
- Какое влияние оказывает.
- Возможные варианты исправления с Вашей точки зрения.

Выплата и размеры наград:

- Минимальная награда: $100.
- Награда прямо пропорционально зависит от серьезности уязвимости и детализации описания в отчете.
- Выплаты производятся только через сервис HackerOne.

полный отказ в выплате награды за нее.

VK Vulnerability Reward Program

The scope of this program is limited to finding technical vulnerabilities in VK services and its official mobile apps.

Vulnerabilities are flaws in the system, the intentional exploitation of which can compromise the system's integrity, confidentiality or proper functionality.

For questions not related to this program, please contact our Support team.

Official apps communities:

- VK App for iPhone: https://vk.com/iphone_app
- VK App for Android: https://vk.com/android_app
- VK Admin: https://vk.com/vkadmin
- VK Messenger: https://vk.com/desktop_app

Qualifying Vulnerabilities:

To assess vulnerabilities, we use OWASP Top 10 2017 for web-services and OWASP Mobile Top 10 2016 for mobile.

- Remote Code Execution (RCE)
- SQL Injection
- Local-Remote File Inclusion (LFI/RFI)
- XML External Entity (XXE)
- Broken Authentication (2FA bypass, etc.)
- Sensitive Data Exposure
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Using Components with Known Vulnerabilities (with examples)
- Server Side Request Forgery (SSRF)
- Cross Site Request Forgery (CSRF)
- Insecure Direct Object References (IDOR)
- Open Redirect (not through /away.php)
- Flood-control bypass
- Privacy bypass
- Other Injections

Non-qualifying Vulnerabilities:

- Reports from security scanners and other automated systems.
- Vulnerability reports based solely on software/protocol versions without a valid proof of concept.
- Reports about missing protection mechanisms or mismatched recommendations (for example, the absence of a CSRF token) without referring to a concrete negative consequence.
- Logout CSRF.

- Reports about Open Redirect (through /away.php).
- IDN homograph attacks.
- Disclosure of user/community public information (see privacy settings).
- Attacks that require complete access to a user's page or browser profile.
- Vulnerabilities within partner services and products that are not directly affecting VK's products and services security.

Strictly Prohibited:

- DDoS attacks.
- Social engineering.
- Gaining physical access to the servers/infrastructure.
- Threats/harm to company employees.

Moreover, such actions will be prosecuted to the fullest extent of the law, without exception.

Report Recommendations:

When writing your report, be sure to include the following to increase your chances of receiving a reward.

- The service containing the vulnerability.
- The type of vulnerability.
- Examples of exploiting it, captured by screenshots or screencasts.
- Methods of reproducing the vulnerability.
- What impact the vulnerability has.
- Recommendations for fixing the vulnerability.

Rewards:

- Minimum reward: $100.
- The reward amount depends on the severity of the vulnerability and how detailed the respective report is.
- Payments are only made through HackerOne.
- The reward will only be given to the first researcher that reports a previously unknown vulnerability.
- We consider the exploitation of discovered vulnerabilities to be extremely unethical, and we will not provide a reward in such cases.

Last updated on June 30, 2020. View changes

Scopes

In Scope

Domain	***.vk.com** `vk.com`, `m.vk.com`, `api.vk.com`, `login.vk.com`, `oauth.vk.com`	Critical	

Domain	***.vk.link**	Critical	$ Eligible
Domain	***.vkpay.io** VK Pay: https://vk.com/vkpay	Critical	$ Eligible
Domain	**connect.vk.com** VK Connect: https://connect.vk.com/promo	Critical	$ Eligible
Other	**Content** `*.vkontakte.(ru|com)`, `*.vk-cdn.net`, `*.userapi.com`, `*.vkuser.net`, `*.vkuseraudio.(com|net)`, `*.vkuservideo.(com|net)`, `*.vkuserlive.(com|net)`	Critical	$ Eligible
Android: Play Store	**com.vkontakte.android** VK App: https://vk.cc/android	Critical	$ Eligible
Android: Play Store	**com.vk.im** VK Me: https://vk.com/landings/vkme	Critical	$ Eligible
Android: Play Store	**com.vk.admin** VK Admin: https://vk.cc/adminAndroid	High	$ Eligible
Executable	**VK Messenger** https://vk.cc/messenger	Medium	$ Eligible
iOS: App Store	**564177498** VK App: https://vk.cc/iphone	Critical	$ Eligible
iOS: App Store	**1441659687** VK Me: https://vk.com/landings/vkme	Critical	$ Eligible
iOS: App Store	**1219369741** VK Admin: https://vk.cc/adminIOS	High	$ Eligible

Out of Scope

Domain	***.vk-apps.com**

Download Burp Suite Project Configuration file (14 URLs) View changes Last updated on June 30, 2020.

Response Efficiency

2 hrs

Average time to first response

2 hrs

Average time to resolution

100% of reports

Meet response standards

Based on last 90 days

Program Statistics

Updated Daily

$330,600

Total bounties paid

$6,900

Bounties paid in the last 90 days

98

Reports received in the last 90 days

3 days ago

Last report resolved

841

Reports resolved

453

Hackers thanked

Top hackers



irek

Reputation:2188



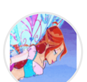
pisarenko

Reputation:948



executor

Reputation:873



povargek

Reputation:700



arfulcat

Reputation:606